SAPIENTIA EDUCATION TRUST

OLD BUCKENHAM HIGH SCHOOL

Achieving excellence together

OLD BUCKENHAM HIGH SHOOL

E-SAFETY POLICY

Author / Edited by	Mr A Fell
Date	March 2019
Executive summary	This policy has been reviewed and amendments made in order to comply with Trust requirements and those of the Local Authority
Review Body	School
Endorsed by	Governing Body
Review frequency & next review due	Every 3 years or as required – March 2022
Comments	This policy is available on our school website and is available on request from the school office. This policy will be reviewed in full by the Governing Body on an annual basis.

Endorsed by **Old Buckenham High School** Governing Body on Monday 18th March 2019

Writing and Reviewing the E-safety policy

The Old Buckenham High School E-safety Policy outlines the school's commitment to ensuring that all stakeholders use the Internet and digital communication safely and responsibly. This policy should be read in conjunction with the data protection policy including GDPR, staff code of conduct, Guidance for Safer Working Practice for adults who work with children and young people in schools (2015) and the school safeguarding/ child protection policy, behaviour policy

- The School will identify a member of staff who has an overview of E-safety; this will be Mr A Dwight (DSL)
- Our E-safety Policy has been written by the School, building on best practice and government guidance. It has been agreed by the senior leadership team and approved by Governors.

Teaching and learning

Why Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the curriculum and a necessary tool for staff and students.
- The school Internet access is provided by TalkTalk and includes filtering appropriate to the age of students.
- Students will be taught what Internet use is acceptable and what is not and given clear objectives and guidance for Internet use.
- Students will be educated in the effective use of the Internet.

Students will be taught how to evaluate Internet content

- The School will seek to ensure that the use of Internet derived materials by staff and by students complies with copyright law.
- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Students will be taught how to report unpleasant or inappropriate Internet content e.g. using the CEOP Report Abuse icon or directly to an adult in school using the school safeguarding procedures.

Managing Internet Access Information system security

- The School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Sapientia Educational Trust

E-mail Communication

- Students and staff may only use approved school e-mail accounts on the school system.
- Students must immediately tell a teacher if they receive an offensive e-mail.
- Students must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission.

- Staff to student email communication must only take place via a school email address and this will be monitored.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school e-mail is supplied through TalkTalk and will control how emails from students to external bodies are presented and controlled.

Published content and the school website

- The contact details on the website will be the school address, e-mail and telephone number. Staff or students' personal information will not be published.
- The Marketing Officer will update the website in line with GDPR.

Publishing photographs, images and work

- Photographs that include students will always be selected carefully, with consent given and meet the requirements of the GDPR
- Students' full names will be avoided on the website or in other school publicity material, as appropriate, including in blogs, forums or wikis, or through Twitter or similar particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs or images of students are published.
- Written permission from adults will be obtained before their names, photographs or images of themselves are published.
- Parents/carers should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic sites.

Social networking and personal publishing

- The school will control access to social networking sites and consider how to educate students in their safe use e.g. use of passwords.
- All users will be advised never to give out personal details of any kind that may identify them, anybody else or their location.
- Students, parents/carers and staff will be advised on the safe use of social network spaces
- Students will be advised to use appropriate nicknames and/ or avatars when using social networking sites.

Managing filtering

- The school will work in partnership with SET to ensure systems to protect students are regularly reviewed and updated.
- If staff or students come across unsuitable on-line materials, the site must be reported to the nominated member of staff.
- The school will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

- Emerging technologies will be examined for their educational benefit and a risk assessment will be carried out before their use in school is allowed.

Other devices

- Students who bring in personal mobile phones, tablets and other SMART devices into school to do so at their own risk. The school does not take any responsibility for the loss or damage of these items.
- The use of personal mobile phones, tablets and other SMART devices and associated cameras are only permitted when authorised by the class teacher or any other member of the school staff.
- The sending of abusive, offensive or inappropriate material is forbidden.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to GDPR and as per the School Data Protection policy.
- Staff must ensure that any data is stored using Office 365, the use of memory sticks, hard drives or similar devices can only be used with permission from the Headteacher.

Policy Decisions

Authorising Internet access

- All staff must read and accept the school Acceptable Use policy document before using any school ICT resource.
- Students must sign to say that the Acceptable Use Policy and the consequences of breaking the Policy have been explained to them and fully understood.
- The school will maintain a current record of all staff and students who are granted access to school ICT systems.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SET can accept liability for the material accessed, or any consequences of Internet access.

- The school will regularly audit its ICT use to establish if the E-safety policy is adequate, appropriate, effective and to ensure that it fully meets all statutory requirements and legislation.

Handling E-safety complaints

- Complaints of Internet misuse will be dealt with by an appropriate senior member of staff within the current school sanctions system.
- Any complaint about staff misuse must be referred to the Headteacher directly.
- Complaints of a safeguarding/ child protection nature must be referred to the DSL Mr A Dwight and will be dealt with in accordance with the school safeguarding procedures.
- Students and parents/carers will be informed of the complaint's procedure.
- Students and parents/carers will be informed of consequences for students misusing school ICT equipment/ Internet.

Community use of the Internet

- All use of the school Internet connection by the community and other organisations shall be in accordance with the school E-safety policy.

Communications of E-Safety

Introducing the E-safety policy to students

- Appropriate and relevant elements of the E-safety policy will be shared with students through Computing lessons.
- E-safety rules will be posted in all networked rooms.
- Students will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for students.
- Assemblies and outside agencies will be used to promote E-safety where appropriate and relevant.

Staff and the E-safety policy

- All staff will have access to the E-safety policy as well as the Acceptable Use policy and its importance explained during their school induction.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.
- Staff who manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues**.**

Enlisting parents' support

- Parents' and carers' attention will be drawn to the School E-safety Policy in newsletters, the school brochure and on the school website.
- Parents/carers will from time to time be provided with additional information on E-safety when and where this is relevant.